UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

– against –

MEMORANDUM & ORDER
24-CR-123 (MKB)

YUE ZHOU,

Defendant.

MARGO K. BRODIE, United States District Judge:

On March 26, 2024, a grand jury returned an indictment charging Defendant Yue Zhou with use of interstate commerce facilities in the commission of murder-for-hire, in violation of 18 U.S.C. § 1958(a). (Indictment ¶ 1, Docket Entry No. 1.) On November 8, 2024, Zhou moved to "suppress all the [Internet Protocol ("IP")] address information the government warrantlessly collected for this case."[1] (Def.'s Mem. 6.) The Government opposed the motion. (Gov't Opp'n 1.)

For the reasons discussed below, the Court denies Zhou's motion to suppress.

I. Background

a. Factual background

The Indictment charges that on or about March 29, 2019, Zhou knowingly and intentionally used a cellular phone and the Internet with the intent that a murder be committed in exchange for money. (Indictment ¶ 1.) The Government contends that Zhou was involved in an

[1] (Def.'s Notice of Mot. to Suppress ("Def.'s Mot."), Docket Entry No. 18; Def.'s Mem. in Supp. of Def.'s Mot. ("Def.'s Mem."), Docket Entry No. 18; Gov't Opp'n to Def.'s Mot. ("Gov't Opp'n"), Docket Entry No. 19; Def.'s Reply in Supp. of Def.'s Mot. ("Def.'s Reply"), Docket Entry No. 20.)

affair with the spouse of her intended victim. (Gov't Opp'n 2.) Zhou allegedly made a $5,000 Bitcoin payment to a hitman website for the murder of her affair partner's spouse and sought to use the same hitman website for the murder of her affair partner's adult daughter. (*Id.* at 2–3.)

On February 19, 2021, Zhou allegedly sent a text message to one of the adult daughter's neighbors to try to hire them to murder the adult daughter. (*Id.* at 3.) After applying for and receiving a search warrant, law enforcement used cell site location information ("CSLI") to determine that the texts were sent from a phone located in Flushing, Queens. (*Id.*) The CSLI also showed that the phone was in Cheyenne, Wyoming, near the intersection of Pioneer Avenue and West 20th Street on January 2 and 3, 2021, and in Flushing, Queens as of January 6, 2021. (*Id.*) Law enforcement agents subpoenaed and obtained information from Expedia Group, Inc. ("Expedia"), a travel booking website, that on January 2, 2021, Zhou booked a flight for January 4, 2021 departing from Denver, Colorado and arriving in New York. (*Id.* at 3, 14, 16.) Expedia's records indicated that the IP address for this booking geolocated to Cheyenne, Wyoming. (*Id.*) Law enforcement "issued process" to Charter Communications, Inc., regarding the IP address, which returned a service address for a spa near Pioneer Avenue and West 20th Street in Cheyenne, Wyoming. (*Id.* at 3–4.) Law enforcement also collected Zhou's IP addresses from other sources, including 88 account logins from Bank of America and 708 account logins from Apple, which geolocated Zhou in cities around the country from January of 2019 to September of 2020.[2] (Def.'s Mem. 8.)

[2] Zhou argues that the Court should "[c]onsider the [c]ollected IP [a]ddress [i]nformation as a [w]hole." (Def.'s Reply 7.) This information includes the two IP address records the Government collected from Expedia showing Zhou's trips in November of 2020 and to and from Denver, Colorado in January of 2021, and the IP address records from Bank of America and Apple. (*Id.*; Def.'s Mem. 8.) The Government represents that it only intends to rely on the two Expedia IP address records and thus Zhou's arguments as to the other records are moot. (Gov't

b. Motion to suppress

On November 8, 2024, Zhou moved to suppress "all warrantlessly collected IP address information." (Def.'s Mem. 1.) In support, Zhou argues that (1) the Government's warrantless collection of Zhou's IP address was a Fourth Amendment search and (2) the Government cannot establish an exception to the Fourth Amendment's warrant requirement. (*Id.* at 9–18.)

The Government argues that Zhou's motion is meritless because (1) the Government permissibly sought, received, and relied on IP addresses obtained without a warrant and (2) Zhou is not entitled to an exclusion of the evidence under prevailing Second Circuit case law. (Gov't Opp'n 4–16.)

II. Discussion

a. Standard of review

"On a motion to suppress, the defendant bears the initial burden of establishing that a government official acting without a warrant subjected him to a search or seizure," *United States v. Davis*, 111 F. Supp. 3d 323, 331 (E.D.N.Y. 2015) (quoting *United States v. Herron*, 18 F. Supp. 3d 214, 221 (E.D.N.Y. 2014)), and that the defendant "had a reasonable expectation of privacy in the place or object searched," *United States v. Delva*, 858 F.3d 135, 148 (2d Cir. 2017). *See also United States v. Lewis*, 62 F.4th 733, 741 (2d Cir. 2023) ("As the proponent of the motion to suppress, it was [defendant]'s burden to establish that the search violated his

---

Opp'n 1–2.) The Court considers Zhou's argument as they relate to evidence the Government intends to offer at trial. *See, e.g.*, *United States v. Morris*, No. 20-CR-100, 2022 WL 1651408, at *12 (W.D.N.Y. Apr. 12, 2022) *report and recommendation adopted*, 2022 WL 1645261 (W.D.N.Y. May 24, 2022) (holding that a motion to suppress is moot where the government represented that they would not rely on information from the search at trial); *United States v. Butler*, No. 15-CR-107, 2017 WL 4324684, at *2 (W.D.N.Y. Sept. 29, 2017) ("[W]hen the government represents that it will not use certain evidence against a defendant, a motion to suppress that evidence is moot.").

Fourth Amendment rights."). Once the defendant has shown a basis for his motion, the burden shifts to the government to demonstrate by a preponderance of the evidence that the search or seizure did not violate the Fourth Amendment. *Delva*, 858 F.3d at 160 (collecting cases); *see also United States v. Iverson*, 897 F.3d 450, 458 (2d Cir. 2018) ("If a defendant has shown that he had a reasonable expectation of privacy in the place or object in question, the government has the burden of showing that the entry, search, or seizure was lawful because it fell within one of the exceptions to the warrant requirement"); *United States v. Chandler*, 164 F. Supp. 3d 368, 376 (E.D.N.Y. 2016) ("[O]nce the [d]efendant shows that the [g]overnment official was acting without a warrant, 'the government has the burden of showing that the search was valid because it fell within one of the exceptions to the warrant requirement' of the Fourth Amendment." (quoting *United States v. Perea*, 986 F.2d 633, 639 (2d Cir. 1993))); *United States v. Wyche*, 307 F. Supp. 2d 453, 457 (E.D.N.Y. 2004) ("On a motion to suppress evidence in a criminal trial, once [the defendant] establishes a basis for his motion, the burden rests upon the [g]overment to prove, by a preponderance of the evidence, the legality of the actions of its officers.").

b. The Court denies Zhou's motion to suppress

The parties do not dispute that the Government did not have a search warrant to collect Zhou's IP addresses. (*See* Gov't Opp'n 1.) The Court thus considers whether (1) Zhou had a reasonable expectation of privacy in the IP addresses and, if so, (2) whether the good faith exception to the exclusionary rule applies. For the reasons explained below, the Court finds that Zhou did not have a reasonable expectation of privacy in her IP address records. While this is alone sufficient to deny her motion to suppress, the Court nevertheless addresses the parties' arguments regarding the applicability of the good faith exception to the exclusionary rule.

i. Zhou did not have a reasonable expectation of privacy in the Expedia IP addresses

First, Zhou argues that she had a subjective expectation of privacy in her IP addresses. (Def.'s Mem. 9–10.) Second, she argues that her expectation of privacy in her IP addresses was objectively reasonable based on the same logic the Supreme Court used to conclude that there is a reasonable expectation of privacy in CSLI in *Carpenter v. United States*, 585 U.S. 296 (2018). (*Id.* at 10–11.) In support, Zhou contends that, like CSLI, IP address location information is "inescapably and automatically created," (*id.* at 11–12), can reveal "large volumes of deeply personal information," (*id.* at 13–15), and "effectively put[s] the entire public under surveillance, not just those the government suspect[s] of a crime" (*id.* at 15–16). Finally, Zhou argues that *Carpenter* abrogated the Second Circuit's conclusion in *United States v. Ulbricht* that an individual does not have a reasonable expectation of privacy in their IP address records, thus "freeing" the Court to conclude that a warrantless collection of IP address records is a Fourth Amendment Violation. (Def.'s Reply 4–6.)

The Government argues that Zhou did not have an objectively reasonable expectation of privacy in her IP addresses.[3] In support, the Government argues that (1) IP addresses are fundamentally different from the CSLI compilations at issue in *Carpenter*, (Gov't Opp'n 7–8), (2) "the law in the Second Circuit is already settled that the government does not need a warrant to obtain IP address information," (*id.* at 8–9), (3) "no court has recognized a legally protected privacy interest in IP addresses," (*id.* at 11), and (4) IP address records, unlike CSLI, are "limited to those websites that the defendant chose to visit and those services that the defendant chose to

[3] The Government does not address Zhou's argument that she had a subjective expectation of privacy in her IP address records. (Gov't Opp'n 7–13.) In her reply, Zhou contends that "the government does not appear to contest that Ms. Zhou had a subjective expectation of privacy in her IP address information." (Def.'s Reply 1.) Accordingly, the Court only addresses whether Zhou had an objectively reasonable expectation of privacy.

engage on the specific dates and specific times she chose to do those things" (*id.* at 12–13).

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ." U.S. Const. amend. IV. "A search occurs when the Government acquires information by either 'physically intruding on persons, houses, papers, or effects,' or otherwise invading an area in which the individual has a reasonable expectation of privacy." *United States v. Ganias*, 755 F.3d 125, 133 (2d Cir. 2014) (citations omitted). "A seizure occurs when the Government interferes in some meaningful way with the individual's possession of property." *Id.* (citations omitted).

Generally, as a threshold matter, there must be a reasonable expectation of privacy in the places or items for there to be a search or seizure within the meaning of the Fourth Amendment. *See California v. Ciraolo*, 476 U.S. 207, 211 (1986) ("The touchstone of Fourth Amendment analysis is whether a person has a 'constitutionally protected reasonable expectation of privacy.'" (citation omitted)); *United States v. Lyle*, 919 F.3d 716, 727 (2d Cir. 2019) ("To prove that a search violated the Fourth Amendment, 'an accused must show that he had a legitimate expectation of privacy in a searched place or item." (quoting *United States v. Rahme*, 813 F.2d 31, 34 (2d Cir. 1987))); *United States v. Simmonds*, 641 F. App'x 99, 104 (2d Cir. 2016) ("It is well established that the Fourth Amendment applies only to spaces in which an individual has a reasonable expectation of privacy."); *Shaul v. Cherry Valley-Springfield Cent. Sch. Dist.*, 363 F.3d 177, 184 (2d Cir. 2004) (finding no search or seizure claim because plaintiff had no reasonable expectation of privacy in personal property maintained in classroom after being suspended); *United States v. Moran*, 349 F. Supp. 2d 425, 467 (N.D.N.Y. 2005) ("[W]here there is no legitimate expectation of privacy, there is no search or seizure within the ambit of the Fourth Amendment." (citation omitted)); *see also Florida v. Jardines*, 569 U.S. 1, 11 (2013)

("The *Katz* [*v. United States*, 389 U.S. 347 (1967),] reasonable-expectations test 'has been *added to*, not *substituted for*,' the traditional property-based understanding of the Fourth Amendment . . . ." (citation omitted)). In assessing the legitimacy of an expectation of privacy, courts employ a "two-part" inquiry from *Katz*: "first, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?" *Ciraolo*, 476 U.S. at 211; *see also United States v. Lyle*, 919 F.3d at 727 ("The person challenging the search must demonstrate a subjective expectation of privacy in the place searched, and that expectation must be objectively reasonable.") (citing *United States v. Paulino*, 850 F.2d 93, 97 (2d Cir. 1988)).

However, there is "no legitimate expectation of privacy in information [an individual] voluntarily turns over to third parties." *United States v. Felder*, 993 F.3d 57, 75 (2d Cir. 2021) (quoting *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979)); *United States v. Miller*, 425 U.S. 435, 443 (1976) (holding that the "Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to [the] Government . . . ."). This "third-party doctrine" does not rely solely on an individual sharing the information with a third party, but instead considers "'the nature of the particular documents sought' to determine whether 'there is a legitimate "expectation of privacy" concerning their contents.'" *Miller*, 425 U.S. at 442. In *United States v. Ulbricht*, the Second Circuit considered two Fourth Amendment issues: whether IP address information was subject to a reasonable expectation of privacy, and whether a particular warrant was overbroad. 858 F.3d 71, 95 (2d Cir. 2017). The Second Circuit concluded that "IP address information and similar routing data, which reveal[ed] the existence of connections between communications devices without disclosing the content of the communications" are "precisely analogous to the capture of telephone numbers at issue in

Smith." *Id.* at 97. In *Smith v. Maryland*, the Supreme Court held that an individual has no reasonable expectation of privacy in the pen register records of the phone numbers they dial when placing a telephone call. 442 U.S. at 743–44. The Second Circuit reasoned in *Ulbricht* that IP address records, like pen registers, require certain "identifying information [to] be disclosed [to third parties] in order to make communication among electronic devices possible." *Ulbricht*, 858 F.3d at 97. The Second Circuit joined the five other circuit courts that had considered this issue in concluding that the government "did not need to obtain a warrant to collect IP address routing information in which [the defendant] did not have a legitimate privacy interest." *Id.*

The Supreme Court considered a similar issue regarding CSLI in *Carpenter v. United States*. In *Carpenter*, the Supreme Court concluded that the collection of CSLI is an exception to the third-party doctrine because CSLI provides "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years," rather than just locating "a person's movement at a particular time." *Carpenter*, 585 U.S. at 315. CSLI "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations'" which "hold for many Americans the 'privacies of life.'" *Id.* at 311 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). The Supreme Court concluded that "when the Government accessed CSLI from the wireless carriers, it invaded [the defendant's] reasonable expectation of privacy in the whole of his physical movements." *Id.* at 313. The Court emphasized that their conclusion was a "narrow one" and did not "disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools," nor did it "address other business records that might incidentally reveal location information." *Id.* at 316.

With the exception of CSLI, *Carpenter* reiterated that an individual assumed the risk that "business records" that are "not confidential communications" and that contain information that is "exposed to [third-party] employees in the ordinary course of business" and used "for a variety of legitimate business purposes" might also be divulged to the government. *Id.* at 308–09 (first quoting *Miller*, 425 U.S. at 440, 442; and then quoting *Smith*, 442 U.S. at 743).

Since *Carpenter*, the Second Circuit has not addressed whether IP addresses are entitled to a reasonable expectation of privacy. (Def.'s Mem. 18; Gov't Opp'n 9–10.) The Court recognizes that the Second Circuit has not explicitly stated which portions of *Ulbricht* survived *Carpenter*. *See, e.g.*, *United States v. Tompkins*, 118 F.4th 280, 287 (2d Cir. 2024) (citing *Ulbricht* for the proposition that "[t]he Fourth Amendment does not require [that search warrants include] a perfect description of the data to be searched and seized" and noting that *Carpenter* abrogated *Ulbricht* "on other grounds"); *United States v. Walker*, No. 18-3506, 2023 WL 3451419, at *3 (2d Cir. May 15, 2023) (same). Even assuming, as Zhou argues, that *Carpenter* abrogated *Ulbricht*'s conclusion about the warrantless collection of IP addresses, the Court concludes that there is no reasonable expectation of privacy in an individual's IP address records. As discussed below, no federal court to have considered this issue after *Carpenter* has concluded that there is a reasonable expectation of privacy in IP address records, and Zhou's arguments fail to persuade the Court otherwise.

Several circuit courts have considered whether IP addresses are entitled to an expectation of privacy since *Carpenter* and all have reached the same conclusion that there is no expectation of privacy in IP addresses. *See, e.g.*, *United States v. Soybel*, 13 F.4th 584, 591–92 (7th Cir. 2021) (concluding an individual has no privacy interest in their "own IP address or the IP addresses of the websites he visits"); *United States v. Brooks*, 841 F. App'x 346, 350 (3d Cir.

2020) (noting that the Third Circuit has long held that there is "no reasonable expectation of privacy in subscriber information", like IP addresses, that is "voluntarily conveyed to third parties." (quoting *United States v. Christie*, 624 F.3d 558, 573–74 (3d Cir. 2010))); *United States v. Trader*, 981 F.3d 961, 968 (11th Cir. 2020) (denying a motion to suppress IP address records because they do not "directly record[] an individual's location."); *United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019) (holding that "an internet user generates the IP address data that the government acquired . . . only by making the affirmative decision to access a website" whereas "every time a cell phone receives a call, text message, or email, the cell phone pings CSLI to the nearest cell site tower without the cell phone user lifting a finger"); *United States v. Wellbeloved-Stone*, 777 F. App'x 605, 607 (4th Cir. 2019), *cert. denied*, 140 S. Ct. 876 (2020) (holding that the defendant "had no reasonable expectation of privacy in his IP address or subscriber information"); *United States v. VanDyck*, 776 F. App'x 495, 496 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 295 (2020) (same); and *United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018) (holding that IP address data "had no bearing on any person's day-to-day movement" and is within the scope of the Fourth Amendment third-party doctrine). Many district courts in this Circuit have likewise concluded that an individual has no reasonable expectation of privacy in their IP address records. *See, e.g.*, *United States v. Herrington*, No. 20-CR-40, 2021 WL 3487992, at *5 (D. Vt. Aug. 9, 2021); *United States v. Hernandez*, No. 19-CR-97, 2020 WL 3257937, at *20 (S.D.N.Y. June 16, 2020); *United States v. Kidd*, 394 F. Supp. 3d 357, 366–67 (S.D.N.Y. 2019); *United States v. Germain*, No. 18-CR-26, 2019 WL 1970779, at *3 (D. Vt. May 3, 2019); *United States v. Therrien*, No. 18-CR-85, 2019 WL 1147479, *3 (D. Vt. Mar. 13, 2019). While these decisions are not binding on the Court, (Def.'s Reply 8–10), as discussed below, Zhou has not offered any arguments to persuade the Court that every federal court to

consider this issue since *Carpenter* has decided it incorrectly.[4] (*Id.*; Gov't Opp'n 11.)

Zhou has not established that she had a reasonable expectation of privacy in her IP address records. As Zhou argues, "most of us cannot go through life without exposing our IP address to a website" because, much like having a cell phone that records CSLI, "Internet access is indispensable to participation in modern society." (Def.'s Mem. 11–12.) However, unlike CSLI, which permits the Government to track a cell phone's location with "near perfect surveillance" even when an individual is not actively using it, *Carpenter*, 585 U.S. at 311–12, an IP address is generated less frequently and only when an individual affirmatively uses a specific website, (Def.'s Reply 2–4). The parties do not dispute that an individual must actively seek out a particular website for a third party to collect the IP address. (Def.'s Reply 2.) In contrast, cellphones "tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features" and there is "no way to avoid leaving behind a trail of location data" except "from disconnecting the phone from the network." *Carpenter*, 585 U.S. at 300–01, 315. Unlike CSLI, which provides "an all-encompassing record of the [cell phone] holder's whereabouts" regardless of whether the holder is actively using their

[4] Two circuit courts of appeal held prior to *Carpenter* that an individual has no reasonable expectation of privacy in IP address records. *United States v. Wheelock*, 772 F.3d 825, 828–29 (8th Cir. 2014) (holding that the Fourth Amendment does not prohibit the government from acquiring names, IP addresses, and other subscriber information from third-party internet service providers); *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008) (holding an individual "has no Fourth Amendment privacy expectation in the subscriber information" they give to third parties).

In addition, while the Sixth Circuit has not directly addressed this issue, at least one district court in that circuit has concluded that there is no reasonable expectation of privacy in IP address records. *See United States v. Popa*, 369 F. Supp. 3d 833, 838 (N.D. Ohio 2019) (holding that an individual did not have a reasonable expectation of privacy in his IP address because he "voluntarily disclosed his subscriber information to [a third party] when he contracted to receive internet service").

phone, *Carpenter*, 585 U.S. at 311, IP addresses disclose "approximate location" *only when* an individual accesses the Internet. (Def.'s Mem. 13.) The Government collected IP address records from Expedia, Bank of America, and Apple, (Def.'s Mem. 6), which are business websites Zhou presumably sought out for their various services. In other words, IP addresses are the type of "business records that might incidentally reveal location information" that *Carpenter* explicitly did not disturb. 585 U.S. at 316; *see also Herrington*, 2021 WL 3487992, at *5 (holding that a defendant had not established a reasonable expectation of privacy in his IP addresses because "unlike CSLI, 'an internet user generates the IP address data . . . only by making the affirmative decision to access a website or application'" (quoting *United States v. Morel*, 922 F.3d 1, 9 (1st Cir. 2019))); *Hernandez*, 2020 WL 3257937, at *20 (holding that the defendant did not show he had a reasonable expectation of privacy in his IP address records because he did not provide "any evidence indicating that his cellphone 'passively generates IP address information for [a website] to collect in a way similar to CSLI,' or that his cellphone consistently conveys 'geographically accurate information that follow's a [person's] day-to-day movements' in a manner similar to CSLI." (second alteration in original) (quoting *Kidd*, 394 F. Supp. 3d at 366–67)); *Germain*, 2019 WL 1970779, at *4 (holding that an individual did not have a reasonable expectation of privacy in IP addresses that companies "maintained . . . as part of their provision of internet services"); and *Therrien*, 2019 WL 1147479, *3 (holding that IP address information was "information that an account holder voluntarily turned over to Google" and was "squarely within the third-party doctrine" such that the defendant "did not possess a reasonable expectation of privacy in the information . . . .").

In addition, the IP address records do not provide an "all-encompassing record" of Zhou's whereabouts. *Carpenter*, 585 U.S. at 311. In *Carpenter*, the government "obtained

12,898 location points cataloging [the defendant]'s movements — an average of 101 data points per day" over 127 days. *Id.* at 302. These data points allowed the Government to track the defendant in *Carpenter* "as if it had attached an ankle monitor to the [defendant]." *Id.* at 312. In contrast, the number of IP address records the Government collected, including those it does not intend to rely on at trial, amounts to only 798 IP addresses over nearly a year. (Def.'s Mem. 8; Def.'s Reply 7.) While the addresses show that Zhou accessed the Internet from various locales across the United States, they locate Zhou's "movement at a particular time" rather than mapping her physical presence at "every day, every moment, over several years." *Carpenter*, 585 U.S. at 315. The IP address records are not the type of "detailed, encyclopedic, and effortlessly compiled" surveillance information that concerned the Supreme Court in *Carpenter*. *Id.* at 309. *See also Hernandez*, 2020 WL 3257937, at *20 (concluding that IP address "do not 'give the Government near perfect surveillance' in a manner similar to CSLI, GPS-trackers, or ankle monitors" because the IP address records "provided an average of less than [ten] data points per day over [twenty-eight] days," which is "significantly fewer data points each day" than CSLI).

Accordingly, the Court concludes that Zhou has not met her burden of showing that she had a reasonable expectation of privacy in her IP address information.

ii. The good faith exception to the exclusionary rule applies

Zhou argues that the Government cannot establish an exception to the warrant requirement of the Fourth Amendment because the good faith exception does not apply. (Def.'s Mem. 16.) First, Zhou argues that the good faith exception does not apply because a reasonable law enforcement agent would have known that *Carpenter* precluded the Government from "compil[ing] an extensive record of retrospective location information by using subpoenas instead of warrants." (*Id.* at 16–17; Def.'s Reply 10–11.) Second, Zhou argues that, although

she is not aware of exactly how the government obtained her IP address records, there is no other obviously applicable exception to the warrant requirement in this case. (*Id.* at 18.)

The Government argues that even if the Court found that the Government should have obtained a warrant to collect Zhou's IP address records, suppression is unwarranted in this case because the good faith exception to the exclusionary rule applies. (Gov't Opp'n 14.) The Government contends that Zhou has not identified a case "repudiat[ing] the use of subpoenas or other non-warrant process[es] to collect IP address information" and thus no "reasonably well trained officer would have known that the search was illegal in light of all of the circumstances." (*Id.* at 15 (quoting *United States v. Smith*, 967 F.3d 198, 212 (2d Cir. 2020)).)

"The fact that a Fourth Amendment violation occurred — *i.e.*, that a search or arrest was unreasonable — does not necessarily mean that the exclusionary rule applies." *United States v. Maher*, 120 F.4th 297, 320 (2d Cir. 2024) (quoting *Herring v. United States*, 555 U.S. 135, 140 (2009)); *United States v. Hightower*, 950 F.3d 33, 36 (2d Cir. 2020) ("[T]he Fourth Amendment does not itself guarantee that evidence unconstitutionally obtained will be withheld from criminal proceedings. . . . Therefore, the exclusionary rule does not apply in a number of contexts.") (citing *United States v. Leon*, 468 U.S. 897, 906 (1984)). Excluding evidence is "a court's 'last resort, not [its] first impulse'" and a court "will suppress illegally obtained evidence 'only where it results in appreciable deterrence' and not when an officer acts in an 'objectively reasonable manner.'" *Id.* (alteration in original) (quoting *Herring*, 555 U.S. at 140–42). "To the extent that application of the exclusionary rule could provide some incremental deterrent, that possible benefit must be weighed against its substantial social costs." *In re 650 Fifth Avenue and Related Properties*, 934 F.3d 147, 162 (2d Cir. 2019) (quoting *Herring*, 555 U.S. 135, 141). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can

meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* (quoting *Herring*, 555 U.S. at 144.)

The good faith exception to the exclusionary rule applies "where officers 'committed a constitutional violation' by acting without a warrant under circumstances that 'they did not reasonably know, at the time, [were] unconstitutional.'" *Maher*, 120 F.4th at 321 (quoting *United States v. Ganias*, 824 F.3d 199, 221–22 (2d Cir. 2016)); *see also Smith*, 967 F.3d at 212 ("[O]ur good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances" (quoting *Herring*, 555 U.S. at 145)); *United States v. Raymonda*, 780 F.3d 105, 118 n.5 (2d Cir. 2015) (concluding that the "basic insight of the *Leon* line of cases" applies "equally to searches conducted with or without a warrant" and that *Leon* requires a government official's actions to be objectively reasonable to warrant the good faith exception). Exclusion should thus be limited to cases of "deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights." *Davis v. United States*, 564 U.S. 229, 238 (2011) (quotation marks omitted); *Smith*, 967 F.3d at 211 ("[T]he exclusionary rule applies only if the police have violated the Constitution deliberately, recklessly, or with gross negligence, or if a constitutional violation is the product of recurring or systemic negligence") (citations omitted). "[W]hen the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force." *In re 650 Fifth Avenue*, 934 F.4th at 162 (quoting *Davis*, 564 U.S. at 238).

The good faith exception applies to law enforcement's collection of IP address records in this case. As the Second Circuit recently stated, courts should "consider not only our own precedents but also those of other courts" in determining whether a warrantless search was

reasonable. *Maher*, 120 F.4th 321 (quoting *Felder*, 993 F.3d at 75–76). As discussed above, every circuit court of appeal and all district courts in the Second Circuit that have considered this issue after *Carpenter* have concluded that an individual does not have a reasonable expectation of privacy in their IP addresses. *See supra* section II.b.i; *see, e.g.*, *Herrington*, 2021 WL 3487992 at *6 (concluding that the Government's reliance on the Stored Communications Act was "objectively reasonable" because "[f]ollowing *Carpenter*, courts continue to hold that IP address data may be subpoenaed without violating the Fourth Amendment."). When the Government obtained Zhou's IP address records, it was thus acting in "objectively reasonable reliance on appellate precedent existing at the time of the search." *United States v. Zodhiates*, 901 F.3d 137, 143 (2d Cir. 2018); *cf. Smith*, 967 F.3d at 212 (applying the good faith exception where "precedent ran both ways" on an issue and thus the Second Circuit "cannot say that a reasonable well-trained officer . . . would have known" that their actions violated the Fourth Amendment). Given that there is no case law indicating that it was "clearly unconstitutional" for the Government to have obtained Zhou's IP addresses through a court order rather than a warrant, law enforcement actions were not "clearly unconstitutional" and suppression is therefore not warranted. *Felder*, 993 F.3d at 75–77 (concluding that it was not "clearly unconstitutional" for the government to seek a court order rather than a warrant to obtain evidence in accordance with the conclusions of all five courts of appeal that had considered the issue at the time); *United States v. Herron*, 762 F. App'x 25, 31 (2d Cir. 2019) (holding that it was not "clearly unconstitutional" for the government to have obtained evidence pursuant to a court order prior to a contrary Supreme Court ruling).

III. Conclusion

For the foregoing reasons, the Court finds that (1) Zhou did not have a reasonable expectation of privacy in her IP address records, and (2) the Government acted on a good faith belief that their conduct was lawful when they obtained Zhou's IP address records without a warrant. The Court therefore denies Zhou's motion to suppress.

Dated: January 16, 2025
Brooklyn, New York

SO ORDERED:

/s MKB
MARGO K. BRODIE
United States District Judge